09/925,031

Express Mail No. EV020612660US

#5

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

00830571.6

Der Präsident des Europäischen Patentamts;
Im Auftrag

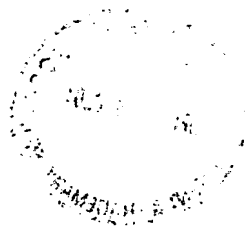
For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 06/08/01
LA HAYE, LE

EPA/EPO/OEB Form 1014 - 02.91



Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 00830571.6
Demande n°:

Anmeldetag:
Date of filing: 09/08/00
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
STMicroelectronics S.r.l.
20041 Agrate Brianza (Milano)
ITALY

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Chaotic encryption

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
H04L9/00

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:
See for original title of the application page 1 of the description

This Page Blank (uspto)

METODO E DISPOSITIVO DI PROTEZIONE DEL CONTENUTO DI UN DOCUMENTO ELETTRONICO

La presente invenzione riguarda un metodo ed un dispositivo di protezione del contenuto di un documento elettronico fornito su un canale trasmissivo.

Come è noto, sin dall'antichità si è presentato il problema di garantire la riservatezza delle informazioni scambiate attraverso mezzi di comunicazione. In generale, tanto più è alto il valore dell'informazione, tanto più essa è appetibile e di conseguenza tanto maggiore deve essere il grado di sicurezza dei mezzi o canali di comunicazione. Quando il canale di comunicazione è di per sé violabile perché facilmente accessibile, la sicurezza della comunicazione deve essere garantita già a monte attraverso la trasformazione dell'informazione in una forma incomprensibile se non ai corretti destinatari dell'informazione. Attualmente, il problema della sicurezza delle informazioni riguarda non solo le comunicazioni attraverso sistemi di telefonia mobile ed Internet, ma anche la trasmissione di documenti testuali o musicali (libri e brani musicali) diffusi per via elettronica su Web o su supporti quali CD e DVD e per i quali sorge il problema di difesa del copyright. In particolare, la protezione del copyright assume importanza

sempre maggiore, visti i grandi interessi economici connessi ai media.

La crittografia si è sempre proposta come la scienza che ha ricercato, nei metodi matematici più robusti, gli algoritmi per tutelare la sicurezza delle comunicazioni, assicurando la trasformazione dell'informazione in una forma incomprensibile, ovviamente permettendo il totale recupero dell'informazione originale ai soggetti autorizzati. Nella valutazione dei sistemi di crittografia, bisogna tenere in considerazione lo scopo che essi si prefiggono. Innanzitutto, è necessario distinguere i tipi di attacco ai quali il sistema crittografico deve opporre resistenza. I tipi di attacco si dividono principalmente in due categorie: attacchi attivi e attacchi passivi. I primi mirano a compromettere l'integrità di un messaggio originario con possibilità, da parte di un ascoltatore indesiderato, di interagire direttamente con le parti mittente e destinatario, allo scopo di utilizzare il canale di comunicazione (erroneamente considerato sicuro dalle parti) per i propri scopi (transazioni, stipula di contratti, intimidazione, atti di pirateria e terrorismo informatico, ecc.). In un attacco passivo, l'utente pirata si limita ad ascoltare e decifrare le informazioni, ritenute segrete, che transitano in un canale in forma crittografata. Un sistema di protezione

del copyright si inserisce in quest'ultimo contesto, dato che lo scopo della protezione è quello di rendere impossibile, ad utenti non autorizzati, la produzione di copie pirata dei documenti protetti.

Attualmente, è sentita l'esigenza di realizzare sistemi di crittografia particolarmente robusti, tenendo conto che la disponibilità di mezzi computazionali sempre più potenti e di risorse di calcolo distribuito ("network computing") ha permesso l'attacco con successo ai più potenti algoritmi di crittografia esistenti, fino a pochi anni fa ritenuti impossibili da "rompere", quali ad esempio il DES (Data Encryption Standard, FIPS 46/77) per il quale sono previste più di $70*10^{15}$ combinazioni di chiavi possibili (56 bit).

I sistemi di crittografia si dividono essenzialmente in due categorie: sistemi a chiave simmetrica e sistemi a chiave pubblica.

Un sistema a chiave simmetrica si basa sull'adozione, da parte del mittente e destinatario, della stessa chiave per la cifratura e successivamente il decrittaggio dell'informazione trasmessa. Questo sistema prevede quindi che, prima che qualsiasi informazione possa essere scambiata, mittente e destinatario debbano definire e/o scambiarsi la chiave ed in seguito cifrare con tale chiave tutte le informazioni da scambiare.

Il vantaggio del sistema a chiave simmetrica consiste nel fatto che il documento crittato può essere decrittato solo da chi è a conoscenza, ed ha la responsabilità di celare, la chiave. Lo svantaggio consiste nel fatto che, qualora più soggetti di un gruppo debbano scambiarsi informazioni tra loro e contemporaneamente mantenerle segrete al resto del gruppo, il numero di chiavi cresce velocemente con il numero di componenti del gruppo. Per n soggetti il numero di chiavi è pari a $n(n-1)/2$.

In un sistema a chiave pubblica, un algoritmo matematico consente l'uso di due chiavi distinte, per crittografare e, rispettivamente, per decrittare un messaggio. Una prima chiave è quindi destinata alla fase di crittografia e viene resa pubblica. Chiunque voglia inviare un messaggio, deve quindi semplicemente prelevare la chiave pubblica del destinatario da un elenco di chiavi pubbliche. Il messaggio così crittato può essere decrittato solo dal destinatario del messaggio, utilizzando una chiave privata, solo a lui nota.

Ciò consente a più mittenti di inviare messaggi cifrati ad un unico destinatario (utilizzando la chiave pubblica) senza che gli altri possibili utenti possano decifrarlo.

Il meccanismo alla base del più famoso algoritmo di

crittografia a chiave pubblica, l'RSA (dal nome degli inventori Rivest, Shamir e Adleman), è la fattorizzazione di numeri con parecchie cifre decimali, per il quale si rimanda alla letteratura.

Il sistema a chiave pubblica ha il vantaggio che solo la chiave privata deve essere tenuta segreta, e il numero di chiavi necessario per lo scambio di informazioni all'interno di una rete è abbastanza contenuto al crescere del numero di utenti (pari a $n(n-1)/2$).

Lo svantaggio consiste nel fatto che le chiavi devono essere necessariamente lunghe, con un numero di bit almeno pari a 512. Ne consegue una rilevante lentezza computazionale, con conseguente basso throughput rate. Inoltre, nessun meccanismo è stato provato come effettivamente sicuro, in quanto non è stata provata l'irresolvibilità della soluzione su cui si basa, la fattorizzazione, anche se questa non è stata mai risolta sin dall'antichità.

Un sistema a chiave pubblica non è utile in un sistema di protezione del contenuto. Infatti, in questo caso, in cui è necessario evitare atti di pirateria sui prodotti multimediali o singolarmente su testi, registrazioni sonore o immagini, è necessario garantire un'alta velocità di decrittaggio. Inoltre, non sarebbe sensato fare scegliere all'utente finale, il destinata-

rio del prodotto multimediale, la coppia di chiavi pubblica e privata.

Il brevetto statunitense 4,434,322, descrive un sistema di trasmissione di dati codificati utilizzabile su un canale di trasmissione che consenta la comunicazione tra due utenti. In questo sistema noto, è implementato un algoritmo di disordinamento ("scrambling") dei dati avente lo scopo di randomizzare l'informazione e nel quale è essenziale garantire la sincronizzazione degli utenti per consentirne la comunicazione. Tale sistema non è quindi adatto per l'applicazione considerata.

Scopo dell'invenzione è quindi mettere a disposizione un sistema di protezione di informazioni trasmesse o memorizzate un supporto elettronico e presentante un elevato grado di sicurezza.

Secondo la presente invenzione viene realizzato un metodo ed un dispositivo di protezione del contenuto di un documento elettronico, come definiti nella rivendicazione 1 e, rispettivamente, 13.

Per la comprensione della presente invenzione ne viene ora descritta una forma di realizzazione preferita, a puro titolo di esempio non limitativo, con riferimento ai disegni allegati, nei quali:

- le figure 1a, 1b, 1c e 1d mostrano differenti diagrammi di un segnale casuale;

- la figura 2 mostra uno schema a blocchi di un dispositivo di crittografia appartenente al presente sistema di protezione;

- la figura 3 mostra uno schema a blocchi del dispositivo di decrittaggio appartenente al presente sistema di protezione;

- la figura 4 mostra l'architettura dei dispositivi di crittografia e decrittaggio delle figure 2 e 3;

- la figura 5 mostra uno schema a blocchi dell'ordinatore/disordinatore di figura 4;

- la figura 6 mostra l'architettura dell'ordinatore/disordinatore di figura 5;

- la figura 7 mostra uno schema a blocchi del generatore caotico di figura 4;

- la figura 8 mostra un diagramma di biforcazione del generatore di mappa caotica di figura 7;

- la figura 9 mostra uno schema di flusso delle operazioni eseguite dall'unità di controllo di figura 4;

- le figure 10a e 10b mostrano la distribuzione di probabilità dei simboli prima e dopo la crittografia di un testo di prova;

- le figure 11a e 11b mostrano la mappatura dei bit di un'immagine originale e della stessa immagine crittografata; e

- la figura 12 mostra la distribuzione di probabi-

lità per le immagini delle figure 11a e 11b.

La presente invenzione utilizza alcune proprietà fondamentale dei segnali generati da circuiti dinamici in evoluzione caotica. Infatti, a chi studia questo particolare tipo di circuiti dinamici non lineari è noto che un circuito in evoluzione caotica è estremamente sensibile alle variazioni imposte, ai parametri che determinano la dinamica complessa e alle condizioni iniziali da cui ha inizio tale dinamica.

In pratica, i segnali generati da due circuiti definiti da parametri prossimi quanto si voglia o da due circuiti identici che evolvano a partire da condizioni iniziali di poco dissimili l'una rispetto all'altra tendono in brevissimo tempo a divergere, evolvendo in modo assolutamente scorrelato nel tempo l'uno rispetto all'altro (sensività ai parametri e alle condizioni iniziali).

L'andamento tipico di un segnale caotico assomiglia molto ad un segnale casuale il cui valore nell'istante $t+\Delta t$ risulta imprevedibile nell'istante t quanto più Δt è grande. Anche dal punto di vista statistico, un processo caotico è, per sua stessa natura, un processo non stazionario e, in particolare non periodico; di conseguenza il suo contenuto in frequenza cambia continuamente la sua distribuzione ("randomness"). L'analisi di un

segnale caotico si avvale spesso di modelli di rappresentazione qualitativi quali, in particolare, i diagrammi di fase o le mappe di Poincaré. Le figure 1a-1d rappresentano tali diagrammi nel caso di un tipico circuito caotico con tre variabili di stato. In particolare, in figura 1a è rappresentato l'andamento dei segnali corrispondenti alle tre variabili di stato nel tempo. La figura 1b riporta un esempio di diagramma delle fasi ottenuto rappresentando una qualsiasi delle variabili di stato $x(t)$ rispetto al valore che la stessa variabile assume all'istante $(t-\tau)$, con τ arbitrario. Nelle figure 1c e 1d sono riportati, infine, gli attrattori in forma di stato che si ottengono rappresentando ciascuna variabile di stato rispetto all'altra (mappe di Poincaré).

Il presente sistema di protezione utilizza inoltre uno schema basato su una fase iniziale di confusione ed una fase successiva di diffusione. Come è noto, il principio di confusione viene soddisfatto attraverso l'uso di trasformazioni che complicano la dipendenza statistica del testo cifrato rispetto alla statistica del testo originale. Il principio di diffusione e' relativo al processo di dispersione dell'influenza di un singolo elemento del testo originale su tutti gli elementi che compongono il documento cifrato (implementato tramite uno stadio disordinatore o "scrambler").

Secondo un aspetto dell'invenzione (figura 2), un cripto-processore 1 comprende uno stadio disordinatore ("scrambler") 2, che implementa la fase di diffusione, ed un elaboratore caotico 3, che implementa la fase di diffusione. Lo stadio disordinatore 2 riceve in ingresso un'informazione da cifrare I e fornisce all'elaboratore caotico 3 un'informazione disordinata I_{DIS}; a sua volta l'elaboratore caotico 3 fornisce in uscita un'informazione cifrata I_{CR}.

L'elaboratore caotico 3 comprende un generatore caotico 5 fornente in uscita un segnale caotico X che viene mescolato all'informazione disordinata I_{DIS} tramite un operatore invertibile. In particolare, il segnale caotico X viene fornito ad una porta di somma esclusiva o porta EXOR 6 ricevente anche l'informazione disordinata I_{DIS} e generante in uscita l'informazione cifrata I_{CR}.

Per la decifratura dell'informazione cifrata I_{CR} è previsto un decripto-processore 10 (figura 3) comprendente un elaboratore caotico 11 ricevente l'informazione cifrata I_{CR} ed un ordinatore 12 fornente in uscita l'informazione decifrata I_{DEC}. L'elaboratore caotico 11, analogamente all'elaboratore caotico 3 di figura 2, comprende un generatore caotico 13 del tutto uguale al generatore caotico 5 (e quindi avente le medesime condizioni di inizializzazione e lo stesso parametro di bi-

forcazione, ed una porta di somma esclusiva o porta EXOR 14, ricevente in ingresso l'informazione cifrata I_{CR} e il segnale caotico X fornito dal generatore caotico 13. Grazie alle proprietà della somma esclusiva o EXOR, l'informazione $I_{DIS'}$ in uscita alla porta EXOR 14 è uguale all'informazione disordinata I_{DIS} in uscita al disordinatore 2 di figura 2; l'ordinatore 12, avente una struttura simile a quella del disordinatore 2 ed utilizzando la stessa chiave (come descritto in seguito) fornisce quindi una informazione decifrata I_{DEC} corrispondente all'informazione originale I.

Il bus collegato fra il disordinatore 2 e l'elaboratore caotico 3 di figura 2 e il bus collegato fra l'elaboratore caotico 11 e l'ordinatore 2 in figura 3 sono inaccessibili, per cui le informazioni presenti su tali bus non sono disponibili per un eventuale attacco di pirateria.

In pratica, il disordinatore 2 del cripto-processore 1, che genera la confusione, genera un testo cifrato il più possibile disturbato, ma invertibile. L'elaboratore caotico 3, addetto alla "diffusione" sottopone il testo disturbato ad una ulteriore fase di cifratura utilizzante un operatore invertibile e valori caotici, incrementando così il livello di sicurezza.

Un esempio dell'architettura del cripto-processore

1 di figura 2 è mostrata in figura 4. In dettaglio, il cripto-processore 1 comprende un'interfaccia di ingresso/uscita 18; un'unità di comando 20; lo stadio disordinatore 2, il generatore caotico 5 e un'area di memoria 21.

L'interfaccia di ingresso/uscita 18 è collegata con l'esterno tramite un bus bidirezionale 19 a 64 bit e con l'unità di comando 20 attraverso una coppia di bus monodirezionali 21a a 16 bit e 21b a 64 bit, sui quali vengono fornite una parola di ingresso IN(t) e una parola cifrata X_{CR_1}; l'unità di comando 20 è collegata con lo stadio disordinatore 2 attraverso una coppia di bus monodirezionali 22a a 16 bit (a cui fornisce la parola di ingresso IN(t)) e 22b a 64 bit (da cui riceve una parola disordinata S_1) e con il generatore caotico 5 attraverso una coppia di bus monodirezionali 23a, 23b a 64 bit su cui vengono forniti un valore caotico precedente X_{i-1} e, rispettivamente, un valore caotico attuale X_i. L'area di memoria 21 comprende una pluralità di locazioni di memoria 24, 25 e 26 in cui sono memorizzati, rispettivamente, un valore caotico iniziale X_0 fornito al generatore caotico 5, un parametro K fornito direttamente al generatore caotico 5, e quattro coefficienti moltiplicativi c_0-c_3 forniti allo stadio disordinatore 2. Ogni coefficiente moltiplicativo c_0-c_3 è formato da 2 byte; insieme,

i coefficienti moltiplicativi c_0-c_3 formano la chiave dello stadio disordinatore 2.

L'unità di comando 20 è costituita da una macchina a stati e comprende un registro 29 nel quale è memorizzato il valore caotico attuale X del segnale caotico; il registro 29 è quindi collegato con la locazione 24 per ricevere, all'inizio della operazioni, il valore iniziale X_0 del segnale caotico X e con il generatore caotico 5, per fornire il valore precedente X_{i-1} calcolato nell'iterazione (i-1)-esima e ricevere il valore X_i calcolato nella i-esima iterazione, come in seguito descritto più in dettaglio. L'unità di comando 20 inoltre invia segnali di comando all'interfaccia 18, al disordinatore 2 e al generatore caotico 5 attraverso un bus di controllo 27, in modo da sincronizzare le operazioni.

Il disordinatore 2, il generatore caotico 5, l'area di memoria 21, l'unità di controllo 20 e tutte le linee che li collegano, ad esclusione dell'interfaccia 18, sono realizzati in un'area protetta ("secret area") di una piastrina di silicio (definente una "smart card") che integra il cripto-processore 1. In particolare l'area protetta è coperta da uno strato di metallizzazione 28 in modo che tutte le operazioni effettuate all'interno dell'area protetta siano celate all'esterno.

Il decripto-processore 10 di figura 3 presenta

un'architettura analoga a quella del cripto-processore 1, tranne per il fatto che il bus 16 è a 64 bit, per i motivi spiegati in seguito.

Lo schema a blocchi del disordinatore 2 e dell'ordinatore 12 è mostrato in figura 5. In dettaglio, il disordinatore 2 comprende quattro sommatori 30a-30d; quattro elementi di ritardo 31a-31d; quattro moltiplicatori 32a-32d; un blocco di trasferimento 33 implementante una funzione di trasferimento di tipo invertibile, ad esempio l'identità h(x)=x; e quattro linee di uscita 34a-34d a 16 bit.

In dettaglio, il sommatore 30a riceve la parola di ingresso IN(t) e l'uscita del sommatore 30b; il blocco di trasferimento 33 è collegato fra l'uscita del sommatore 30a e la linea di uscita 34a; gli elementi di ritardo 31a-31d sono realizzati con registri a scorrimento a 16 bit e sono disposti in cascata uno all'altro e al blocco di trasferimento 33; i moltiplicatori 32a-32c sono collegati ciascuno fra l'uscita di un rispettivo elemento di ritardo 31a-31c e un ingresso di un rispettivo sommatore 30b-30d mentre il moltiplicatore 32d è disposto fra l'uscita dell'elemento di ritardo 31d ed un secondo ingresso del sommatore 30d; e i sommatori 30b e 30c hanno un secondo ingresso collegato con l'uscita del sommatore 30c, rispettivamente 30d.

Tutte le linee del disordinatore 2 mostrate sono a 16 bit e le quattro linee di uscita 34a-34d insieme formano il bus monodirezionale 23b su cui viene fornito un blocco di 64 bit costituente una parola disordinata S_i.

Nel disordinatore 2 di figura 5, le operazioni di somma e di moltiplicazione sono definite all'interno di un campo di Galois (operatore somma con modulo). Gli elementi di ritardo 31a-31b shiftano, ad ogni ciclo di clock, stringhe di caratteri disordinati s(t)÷s(t-3) di 16 bit fornite inoltre alle linee di uscita 34a-34b. All'inizio dell'elaborazione di un documento o testo, ogni elemento di ritardo 31a-31d è inizializzato con due rispettivi byte c_0-c_3 della chiave del cripto-processore 1, forniti dall'area di memoria 21 (figura 4). In fase di inizializzazione, i moltiplicatori 32a-32d ricevono anch'essi due rispettivi byte c_0-c_3 della chiave, che rappresentano i coefficienti moltiplicativi con cui vengono moltiplicate le stringhe di caratteri disordinati s(t-1)÷s(t-4) shiftate dagli elementi di ritardo 31a-31d.

Ad ogni ciclo di elaborazione, i 64 bit di una parola da cifrare I_i vengono forniti, in 4 passi successivi da 16 bit, al disordinatore 2 (parola di ingresso IN(t)). In ciascun passo, ciascuna stringa di caratteri disordinati s(t-1)÷s(t-4) (inizialmente costituita dai 2

byte della chiave memorizzati negli elementi di ritardo 31a-31d) viene moltiplicata per il relativo parametro c_j e del risultato a 32 bit vengono scartati i 16 bit più significativi, realizzando in tal modo una somma con modulo, ovvero una somma definita in un campo di Galois. Le parole cosi' ottenute vengono quindi sommate alla parola di ingresso IN(t), ottenendo man mano un decremento sostanziale del livello di correlazione.

Nei cicli successivi, inoltre, si ha un mescolamento fra le stringhe di caratteri disordinati s(t)÷s(t-3) del ciclo precedente con i blocchi di successive parole da cifrare, aumentando il livello di scorrelazione.

Il disordinatore 2 è, dunque, un sistema non lineare dalle caratteristiche caotiche che genera in uscita un blocco di 64 bit (parola disordinata S_i), la cui distribuzione statistica risulta indipendente da quella del blocco di ingresso (parola da cifrare I_i, figura 4).

L'ordinatore 12 di figura 3 ha la stessa struttura del disordinatore 2 mostrata in figura 5, tranne per il fatto che il sommatore 30a che riceve la parola di ingresso IN(t) è sostituito da un sottrattore, che sottrae dalla parola di ingresso IN(t) la parola fornita dall'uscita del sommatore 30b, in modo da fornire in uscita (sulle linee di uscita 34a-34d) una parola decifrata I_{DECi}.

La figura 6 mostra l'architettura preferita del disordinatore 2. In figura 6, nella quale sono stati utilizzati gli stessi numeri di riferimento della figura 5, i moltiplicatori 32a-32d moltiplicano le parole ritardate in uscita dagli elementi di ritardo 31a-31d con i coefficienti moltiplicativi c_0-c_3 memorizzati in registri 35; inoltre sono evidenziati un segnale di comando SH che determina lo scorrimento verso il basso del contenuto dei registri T costituenti gli elementi di ritardo 31a-31d e un segnale di comando OP che seleziona la funzione di somma o sottrazione del blocco 30a a seconda del funzionamento come disordinatore 2 o ordinatore 12.

La figura 7 mostra lo schema a blocchi del generatore caotico 5. Il generatore caotico 5 è costituito da una logica combinatoria comprendente un primo ed un secondo moltiplicatore 37, 38 ed un sottrattore 39. In dettaglio, il primo moltiplicatore 37 presenta due ingressi riceventi rispettivamente il parametro K dalla locazione di memoria 25 e il valore caotico precedente X_{i-1} dal registro 29 (figura 4) ed un'uscita (a 128 bit) collegata ad un ingresso del secondo moltiplicatore 38; il sottrattore 39 presenta un primo ingresso ricevente il valore caotico precedente X_{i-1}, un secondo ingresso ricevente un valore "1", normalizzato a 64 bit, ed un'uscita (a 128 bit) collegata al secondo ingresso del

secondo moltiplicatore 38; l'uscita del secondo moltiplicatore 38, a 64 bit, fornisce, sulla linea 23b, il valore caotico attuale X_i di 64 bit.

Il generatore caotico 5 implementa la funzione $f_k(x) = Kx(1-x)$, con 0<x<1 e 3,6<K<4, dove K rappresenta il parametro di biforcazione del sistema caotico. Tale funzione (si veda fig. 8) garantisce che i valori caotici X_j definiscano una sequenza scorrelata, che viene quindi utilizzata per cifrare la parola disordinata S_i fornita dal disordinatore 2.

La figura 9 mostra uno schema di flusso delle operazioni svolte dal cripto-processore 1 e controllate dall'unità di controllo 20, che, come si è detto, è preferibilmente realizzata come macchina a stati.

All'inizio, l'unità di controllo 20 viene attivata al ricevimento di un segnale di reset che ne determina l'inizializzazione (fase 50). Al ricevimento del segnale di reset, l'unità di controllo 20 carica dall'area di memoria 21 le chiavi del sistema negli appositi registri: i parametri c_j vengono caricati nei registri costituenti i elementi di ritardo 31a-31d (figure 5 e 6) e nei registri 35 (figura 6), mentre il valore caotico iniziale X_0 viene caricato nel registro 29 dell'unità di controllo 20 (fase 51). Un segnale di orologio, non mostrato, scandisce gli eventi e sincronizza l'intero

cripto-processore 1.

Ad ogni impulso di clock, l'unità di controllo 20 acquisisce, attraverso l'interfaccia I/O 18 una parola di ingresso IN (t) di 16 bit e la invia al disordinatore 2, fase 53. Il disordinatore 2 provvede quindi a sommare la parola di ingresso IN(t) ai prodotti tra i coefficienti c_j ed il contenuto degli elementi di ritardo 31a-31d, come spiegato in precedenza con riferimento alla figura 4 (fase 54). Al ricevimento del segnale di controllo SH fornito dalla unità di controllo 20, il contenuto degli elementi di ritardo 31a-31d scorre inoltre verso il basso. Dopo quattro iterazioni (uscita SI dal blocco 55), un blocco da 64 bit e' stato disordinato e viene fornito all'unità di comando 20 come parola disordinata S_i, fase 56.

Quindi, l'unità di controllo 20 comanda il generatore caotico 5 perché calcoli un nuovo valore caotico attuale X_i. A tale scopo, essa fornisce il valore caotico precedente X_{i-1} al generatore caotico 5, fase 60; il generatore caotico 5 calcola il valore caotico attuale X_i, fase 61, e lo fornisce all'unità di controllo 20 che lo memorizza nel registro 29 al posto del valore precedente X_{i-1}, fase 62.

Quindi l'unità di controllo 20 calcola la parola cifrata $X_{CR,i}$ eseguendo l'xor fra la parola disordinata S_i

e il valore caotico attuale X_i, fase 63, e fornisce il risultato (parola cifrata $X_{CR,i}$) all'interfaccia I/O 18, fase 64.

La sequenza di operazioni descritte, dalla fase 52 fino alla fase 64, continua fino a quando dall'esterno vengono forniti blocchi di parole da cifrare I_i, uscita NO dal blocco 65; quindi termina.

Il cripto-processore 1 descritto è stato sottoposto a simulazione allo scopo di studiare il grado di sicurezza del sistema dal punto di vista della ciclicità e dell'indice di coincidenza utilizzando un testo campione in lingua italiana.

Applicando il presente metodo di crittografia come algoritmo crittografico ad un testo campione in lingua è stato calcolato l'indice di coincidenza su un alfabeto di 256 simboli (codice ASCII); l'applicazione della formula di Friedman (k-test) al testo ha fornito un valore di I = 0,003873, appena superiore del minimo teorico (Imin = 0,003607). Un test ancora più' critico e' stato effettuato su un testo formato dalla ripetizione di un unico carattere. Il risultato di tale test fornisce un indice pari a I = 0,003906, mentre il minimo teorico e' Imin = 0,003900. In figura 10a sono riportate le distribuzioni percentuali di 256 simboli in un testo formato dalla ripetizione di un unico carattere e la figura 10b

mostra le distribuzioni percentuali dei simboli dopo la cifratura con il metodo descritto.

Un'ulteriore valutazione e' stata effettuata prendendo in considerazione un'immagine bitmap (figura 11a); in tale caso si e' ottenuto un indice I = 0,003907 a fronte di un Imin = 0,003890. Come osservabile in figura 11b (relativo alla immagine di figura 11a dopo la cifratura) il contenuto informativo e' completamente disperso. L'immagine ottenuta dopo il processamento risulta infatti completamente scorrelata, come evidenziato nelle distribuzioni percentuali dei simboli in figura 12, in cui la curva A si riferisce all'immagine originale di figura 11a e la curva B si riferisce all'immagine cifrata di figura 11b.

I vantaggi ottenibili con il metodo e il dispositivo descritti sono i seguenti. In primo luogo, come sopra discusso, il metodo e il dispositivo forniscono testi cifrati ad elevata sicurezza. Il fatto di utilizzare una chiave di tipo simmetrico (costituita dal parametro di biforcazione K e dal valore iniziale X_0), memorizzata in un'area inaccessibile, elimina i problemi di sincronizzazione presenti nei sistemi a chiave pubblica. Ciò consente quindi la crittografia di testi e documenti che possono anche essere inviati su rete pubblica (Internet) o forniti su supporto elettronico, dato che la chiave

può essere fornita da un venditore solo al relativo cliente. Il sistema di criterio comprende quindi un lettore (come un DVD) ed un supporto (ad esempio una smart-card) e permette di proteggere il contenuto di documenti protetti da copyright, senza il rischio che utenti non abilitati (che non possiedono la chiave) possano accedere al contenuto decifrato.

Risulta infine chiaro che al metodo e al dispositivo qui descritti ed illustrati possono essere apportate numerose modifiche e varianti, tutte rientranti nell'ambito del concetto inventivo, come definito nelle rivendicazioni allegate.

RIVENDICAZIONI

1. Metodo di protezione del contenuto di un documento elettronico, caratterizzato dal fatto di comprendere le fasi di:

confondere caratteri appartenenti ad un documento elettronico di ingresso (I) attraverso un disordinatore invertibile (2) per ottenere un documento confuso (I_{DIS}); e.

diffondere (3) detto documento confuso per mescolamento con caratteri caotici (X), per ottenere un documento cifrato (I_{CR}).

2. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detta fase di confondere comprende eseguire operazioni definite all'interno di un campo di Galois.

3. Metodo secondo la rivendicazione 1 o 2, in cui detto documento elettronico di ingresso (I) comprende una pluralità di stringhe di caratteri da cifrare (IN) e detto documento confuso (I_{DIS}) comprende una pluralità di stringhe di caratteri confusi (s), caratterizzato dal fatto che detta fase di confondere comprende sommare ciascuna stringa di caratteri da cifrare (IN) con stringhe di caratteri di confusione ottenute moltiplicando dette stringhe di caratteri confusi (s) per rispettive costanti moltiplicative (c_j).

4. Metodo secondo la rivendicazione 3, caratterizzato dal fatto che, prima di essere moltiplicate per dette costanti moltiplicative (c_j), dette stringhe di caratteri confusi (s) vengono ritardate.

5. Metodo secondo una qualsiasi delle rivendicazioni precedenti, in cui detto documento confuso (I_{DIS}) comprende una pluralità di stringhe di caratteri confusi (s), caratterizzato dal fatto che detta fase di diffondere comprende generare caratteri caotici (X) tramite un generatore caotico (5) e mescolare dette stringhe di caratteri confusi (s) con detti caratteri caotici (X).

6. Metodo secondo la rivendicazione 5, caratterizzato dal fatto che detta fase di mescolare comprende eseguire una operazione di or esclusivo (6).

7. Metodo secondo la rivendicazione 5 o 6, caratterizzato dal fatto che detto generatore caotico (5) implementa la funzione:

$$f_k(x) = Kx(1-x) .$$

8. Metodo secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto di comprendere, in sequenza, le fasi di:

a) caricare (51) chiavi di cifratura (c_j) in registri di scorrimento (35) di detto disordinatore invertibile (2) e un valore caotico iniziale (X_0) in un registro di valore caotico (29);

b) acquisire (53) una stringa di caratteri di ingresso (IN);

c) calcolare (54) una stringa di caratteri diffusi (s(t)) utilizzando detta stringa di caratteri di ingresso, dette chiavi di cifratura (c_j) e il contenuto di detti registri di scorrimento (35);

d) alimentare detta stringa di caratteri diffusi (s(t)) a detti registri di scorrimento comandando una operazione di scorrimento di detti registri di scorrimento;

e) ripetere dette fasi b), c) e d) un prefissato numero di volte per ottenere una pluralità di dette stringhe di caratteri confusi (S_i);

f) calcolare (61) un valore caotico successivo (X) utilizzando il contenuto di detto registro di valore caotico (29);

g) sommare (63) detta pluralità di stringhe di caratteri confusi (S_i) con detto valore caotico successivo (X) per ottenere una parola cifrata (X_{CR});

h) memorizzare (62) detto valore caotico successivo in detto registro di valore caotico (35); e

i) ripetere dette fasi b)-h).

9. Metodo secondo la rivendicazione 8, caratterizzato dal fatto che detta fase c) utilizza la seguente relazione:

$$s(t) = IN(t) \oplus \sum_{j=0} c_j \oplus s(t-j)$$

in cui *IN(t)* è detta stringa di caratteri di ingresso, c_j sono dette chiavi di cifratura, *s(t-j)* sono i contenuti di detti registri di scorrimento (35) e *s(t)* è detta stringa di caratteri diffusi.

10. Metodo secondo la rivendicazione 8 o 9, caratterizzato dal fatto che detta fase f) utilizza la seguente relazione:

$$f_k(x) = Kx(1-x),$$

in cui K è un parametro di biforcazione di un sistema caotico.

11. Metodo di sprotezione del contenuto di un documento elettronico protetto tramite il metodo secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto di decifrare detto documento cifrato tramite mescolamento (11) con detti caratteri caotici (X) e ordinamento tramite un ordinatore (12) opposto a detto disordinatore (2).

12. Metodo di sprotezione del contenuto di un documento elettronico protetto tramite il metodo secondo la rivendicazione 3, in cui detto documento cifrato (I_{CR}) comprende una pluralità di stringhe di caratteri cifrati, caratterizzato dal fatto di decifrare detto documento cifrato tramite una prima (11) ed una seconda operazione di decifratura in cascata (12), detta seconda ope-

razione di decifratura (12) fornendo una pluralità di stringhe di caratteri decifrati, detta prima operazione (11) di decifratura comprendendo una fase di mescolamento, in cui dette stringhe di caratteri cifrati vengono mescolate con detti caratteri caotici (X) per ottenere una pluralità di stringhe di caratteri predecifrati ($I_{DIS'}$), e detta seconda operazione di decifratura comprende una fase di ordinamento tramite sottrazione (30a) di ciascuna stringa di caratteri precifrati con stringhe di caratteri di retroazione ottenute moltiplicando dette stringhe di caratteri decifrati per dette costanti moltiplicative (c_j).

13. Dispositivo di protezione del contenuto di un documento elettronico, caratterizzato dal fatto di comprendere:

un blocco di confusione (2) di un documento elettronico di ingresso (I), detto blocco di confusione comprendendo un disordinatore invertibile (2) fornente un documento confuso (I_{DIS}); e

un blocco di diffusione (3) disposto in cascata a detto blocco di confusione, detto blocco di diffusione comprendendo mezzi di mescolamento (6) di detto documento confuso con caratteri caotici (X), fornenti un documento cifrato (I_{DEC}).

14. Dispositivo secondo la rivendicazione 13, ca-

ratterizzato dal fatto che detto disordinatore (2) comprende operatori agenti all'interno di un campo di Galois.

15. Dispositivo secondo la rivendicazione 13 o 14, caratterizzato dal fatto che detto disordinatore (2) comprende un elemento sommatore (30a) avente un primo ed un secondo ingresso, detto primo ingresso ricevendo una stringa di caratteri da cifrare (IN) appartenenti a detto documento elettronico di ingresso (I); una pluralità di registri di scorrimento (31a-31d) disposti in cascata fra loro e a detto elemento sommatore; una pluralità di elementi moltiplicatori (32a-32d), ciascuno avente un ingresso collegato ad un'uscita di un rispettivo registro di scorrimento (31a-31d) ed una propria uscita; una pluralità di nodi sommatori (30b-30d) collegati in cascata, ciascun nodo sommatore avendo un ingresso collegato a detta uscita di un rispettivo elemento moltiplicatore (32a-32c), un nodo sommatore (30d) posto a monte avendo un secondo ingresso collegato ad un ultimo di detti elementi moltiplicatori (31d) ed un nodo sommatore (30b) posto a valle avendo un'uscita collegata a detto secondo ingresso di detto elemento sommatore (30a).

16. Dispositivo secondo una qualsiasi delle rivendicazioni 13-15, caratterizzato dal fatto che detti mezzi di mescolamento (6) comprendono un operatore di somma

logica esclusiva e dal fatto che detto blocco di diffusione comprende un generatore caotico (5).

17. Dispositivo secondo la rivendicazione 16, caratterizzato dal fatto che detto generatore caotico (5) implementa la seguente funzione:

$$f_k(x) = Kx(1-x),$$

in cui K è un parametro di biforcazione di un sistema caotico.

18. Dispositivo secondo una qualsiasi delle rivendicazioni 13-15, caratterizzato dal fatto di comprendere, integrati in una prima piastrina, un'unità logica di comando (20), un'unità disordinatrice (2) collegata a detta unità logica di comando, un generatore caotico (5) collegato a detta unità logica di comando, un'area di memoria segreta (21), memorizzante chiavi di cifratura (c_j) per detta unità disordinatrice (2) ed un valore caotico iniziale (X_0) per detto generatore caotico (5).

19. Dispositivo di sprotezione (10) del contenuto di un documento elettronico cifrato fornito da un dispositivo di protezione (1) secondo una qualsiasi delle rivendicazioni 13-18, caratterizzato dal fatto di comprendere, integrati in una seconda piastrina, un'unità logica di comando (20), un'unità ordinatrice (12) collegata a detta unità logica di comando, un generatore caotico (13) collegato a detta unità logica di comando, un'area

di memoria segreta (21), memorizzante chiavi di cifratura (c_j) per detta unità ordinatrice (12) ed un valore caotico iniziale (X_0) per detto generatore caotico.

20. Dispositivo secondo le rivendicazioni 18 e 19, caratterizzato dal fatto che dette prima e seconda piastrina comprendono ciascuna una metallizzazione di copertura (28) coprente una rispettiva unità logica di comando (20), una rispettiva unità disordinatrice/ordinatrice (2, 12), un rispettivo generatore caotico (5, 13) e una rispettiva area di memoria segreta (21).

RIASSUNTO

Per proteggere il contenuto di un documento elettronico tramite un sistema di crittografia basato su una fase iniziale di confusione in un disordinatore ed una fase successiva di diffusione in un elaboratore caotico, entrambe di tipo caotico, inizialmente vengono acquisite (51) chiavi di cifratura (c_j) ed un valore caotico iniziale (X_0); vengono acquisite (53) stringhe di caratteri di ingresso (IN); vengono calcolate (54) stringhe di caratteri diffusi (s(t)) utilizzando le stringe di caratteri di ingresso, le chiavi di cifratura (c_j) e precedenti stringhe di caratteri diffusi (s(t-j)). Dopo un certo numero di iterazioni, gruppi di stringhe di caratteri diffusi (S_i) vengono sommate (63) a valori caotici successivi (X) generati da un elaboratore caotico (61) per ottenere parole cifrate (X_{CR}). La decifratura avviene attraverso due operazioni successive, in cui le parole cifrate vengono sommate a valori caotici identici a quelli di cifratura (X) e sottratte a parole decifrate in precedenza utilizzando un elemento ordinatore avente struttura simile a quella del disordinatore e utilizzante identiche chiavi di cifratura.

Figura 9

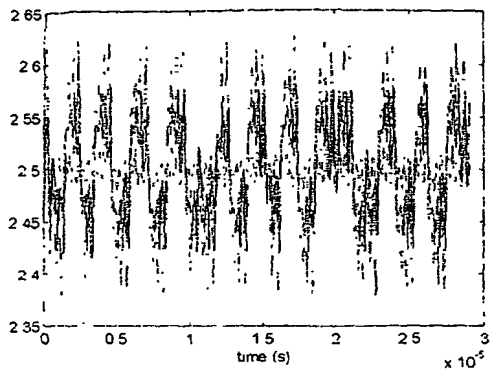


Fig.1a

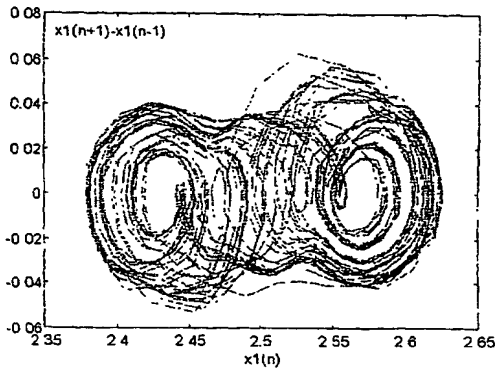


Fig.1b

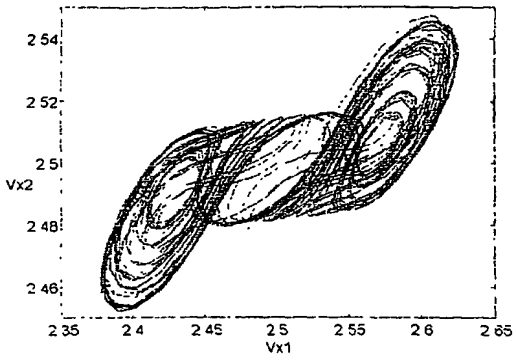


Fig.1c

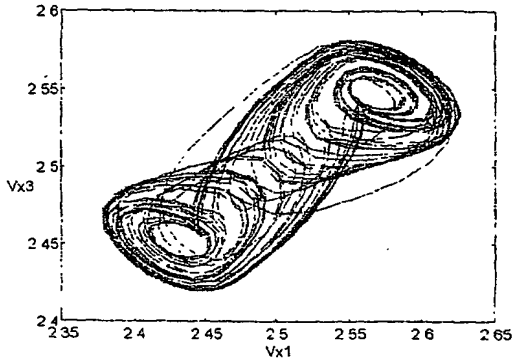


Fig.1d

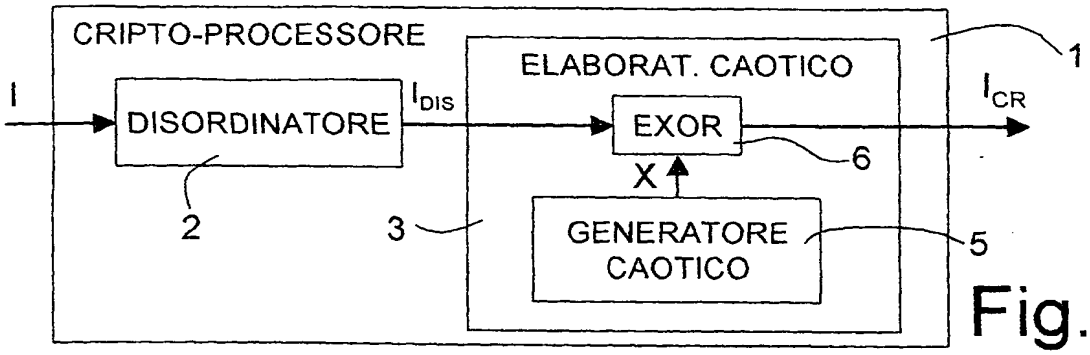


Fig.2

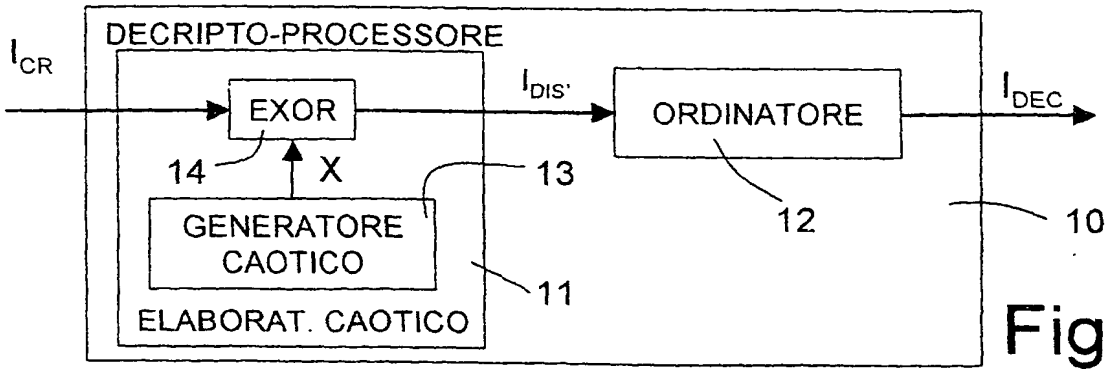


Fig.3

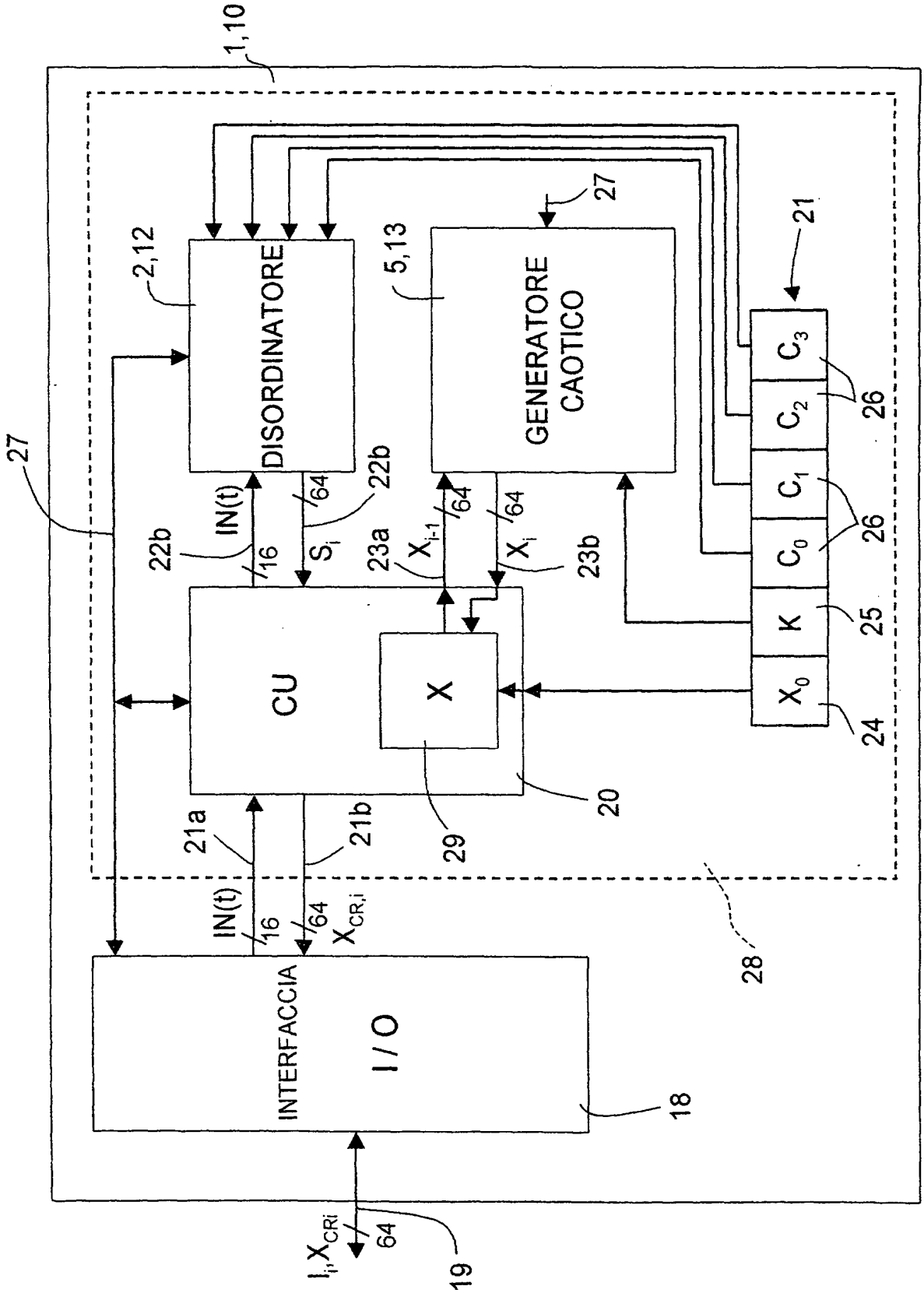

1,10
2,12
DISORDINATORE
5,13
GENERATORE CAOTICO
27
21
C_3
C_2
C_1
C_0
K
X_0
26
25
24
CU
X
20
29
IN(t)
16
64
S_i
22b
23a
X_{i-1}
X_i
23b
21a
21b
$X_{CR,i}$
28
INTERFACCIA I / O
18
I_i, X_{CRi}
19

Fig.4

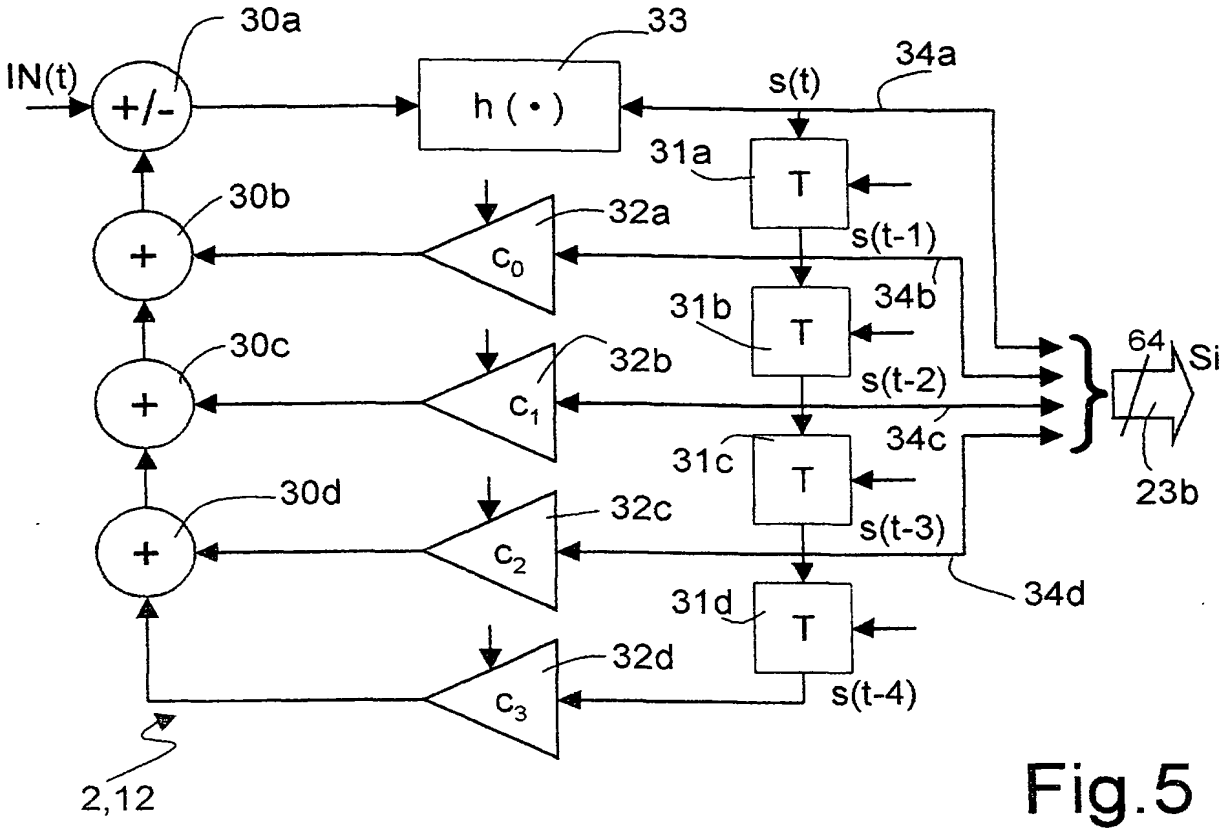

IN(t)
+/-
30a
h (•)
33
s(t)
34a
31a
T
s(t-1)
30b
+
c0
32a
34b
31b
T
s(t-2)
30c
+
c1
32b
64
Si
34c
31c
T
23b
s(t-3)
30d
+
c2
32c
34d
31d
T
s(t-4)
c3
32d
2,12

Fig.5

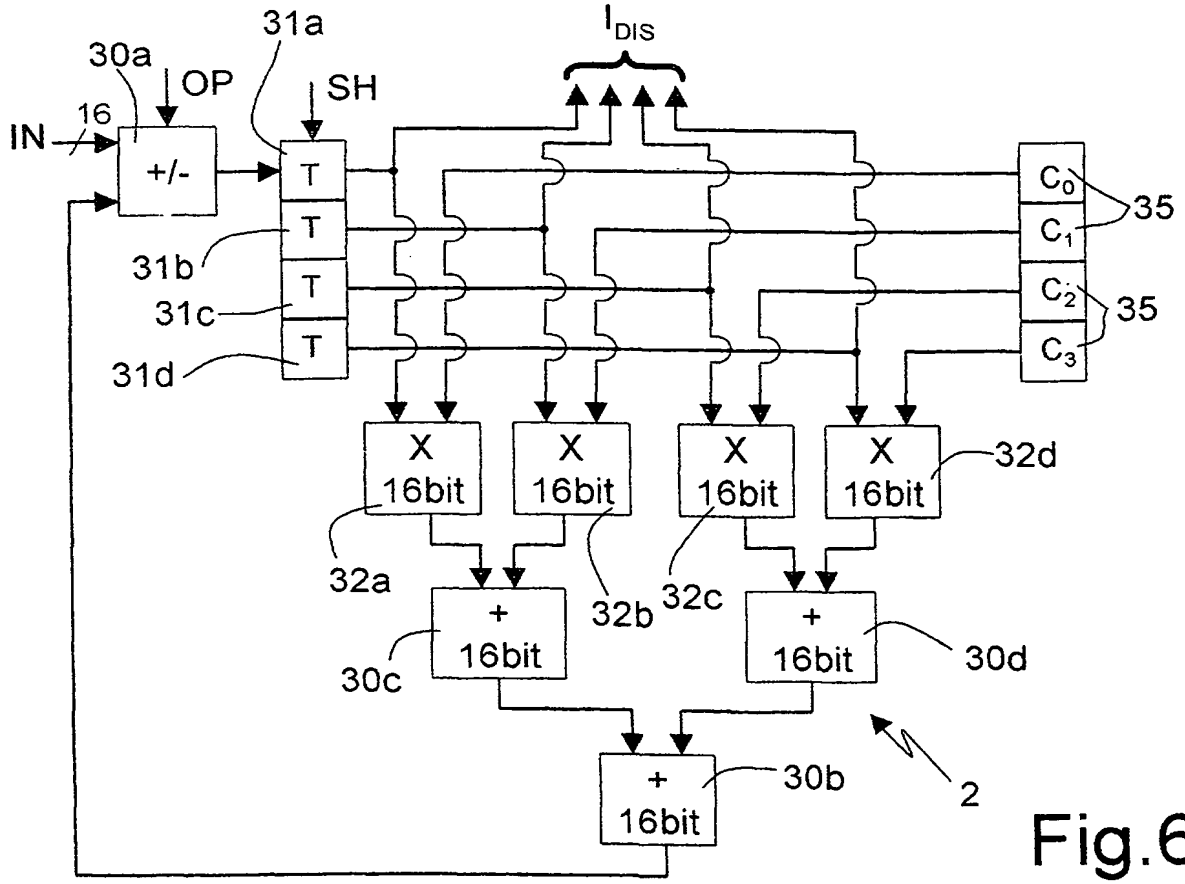

IDIS
31a
30a
OP
SH
IN
16
+/-
T
T
T
T
31b
31c
31d
C0
C1
C2
C3
35
35
X
16bit
32d
32a
32b
32c
+
16bit
30c
30d
30b
2

Fig.6

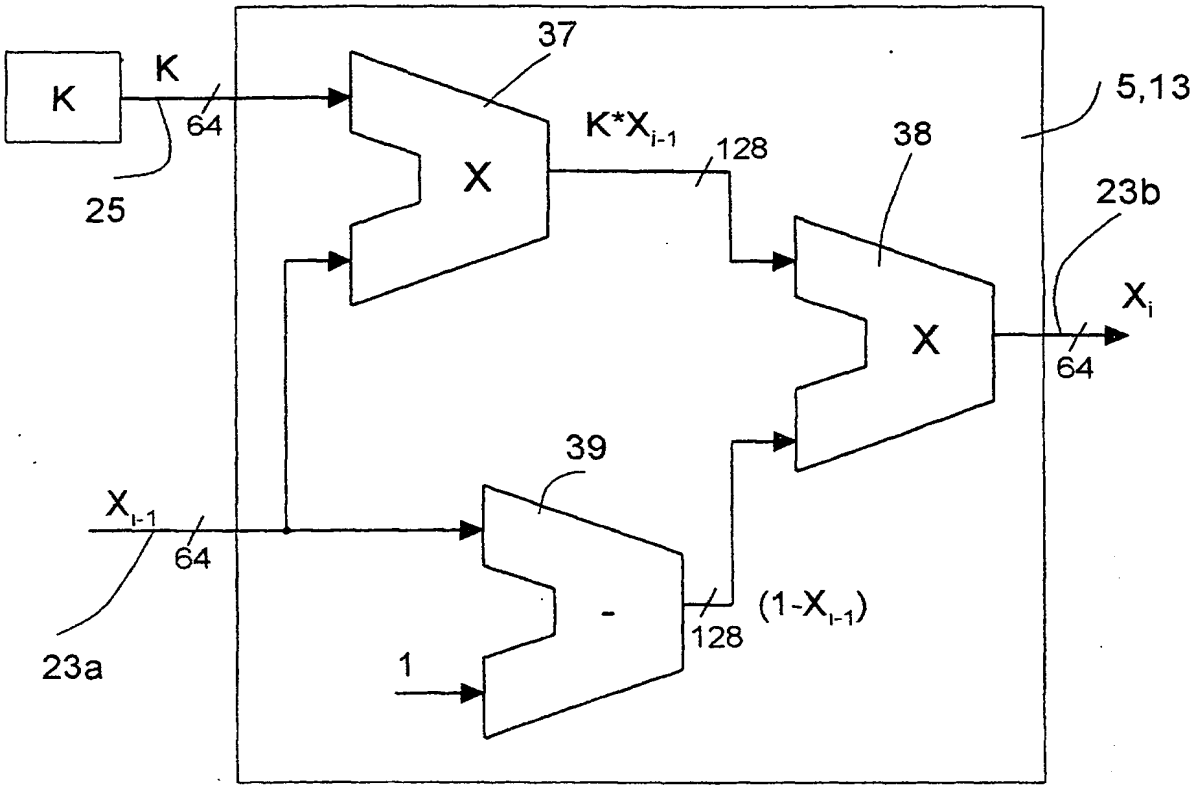

K
K
64
25
37
X
$K*X_{i-1}$
128
38
5,13
23b
X_i
X
64
39
X_{i-1}
64
23a
-
128
$(1-X_{i-1})$
1

Fig.7

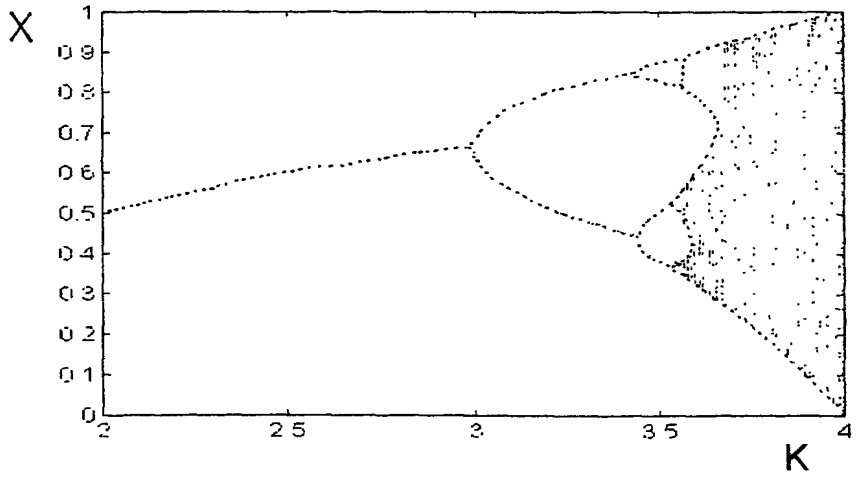

X
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
2
2.5
3
3.5
4
K

Fig.8

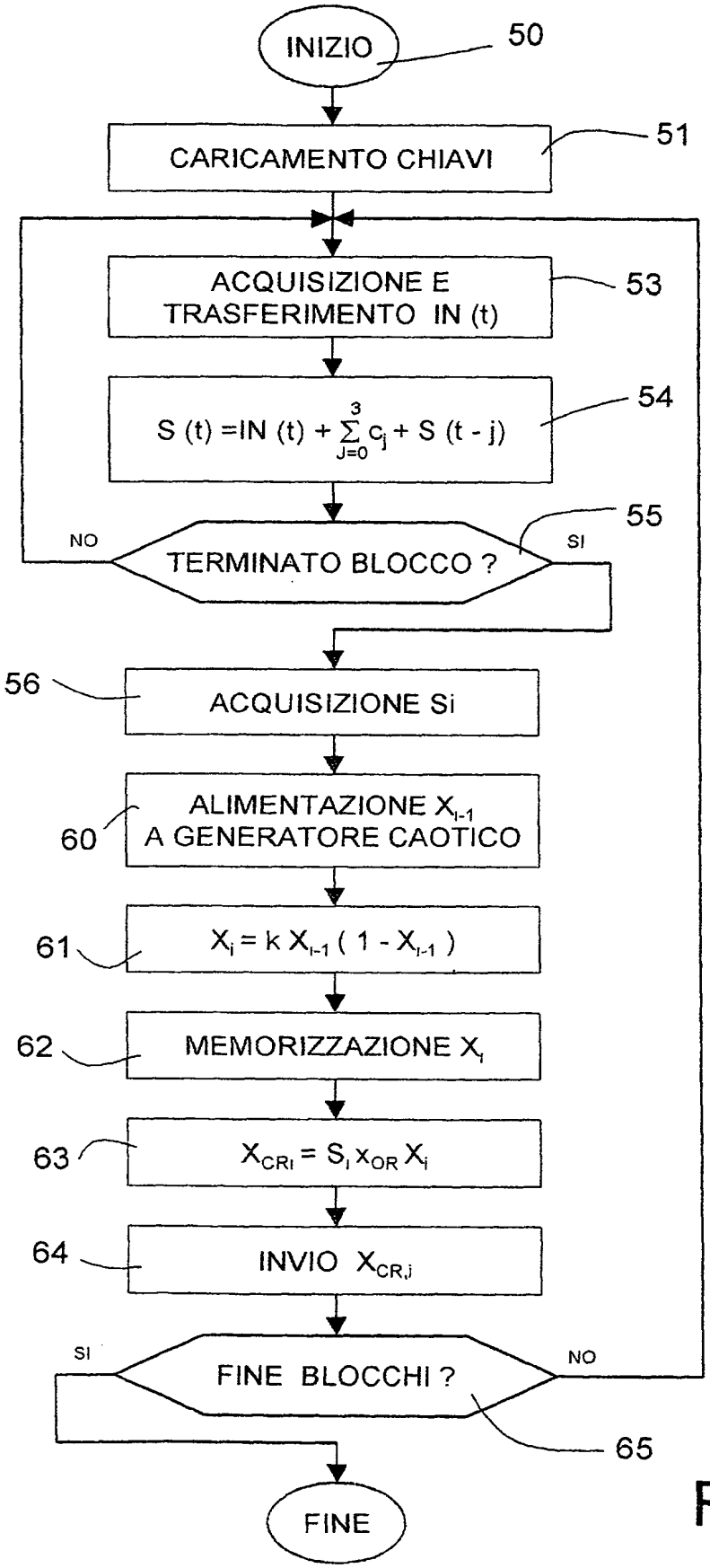

INIZIO
50
CARICAMENTO CHIAVI
51
ACQUISIZIONE E TRASFERIMENTO IN (t)
53
S (t) =IN (t) + $\sum_{J=0}^{3} c_j$ + S (t - j)
54
NO
TERMINATO BLOCCO ?
SI
55
56
ACQUISIZIONE Si
ALIMENTAZIONE X_{i-1} A GENERATORE CAOTICO
60
$X_i = k X_{i-1} (1 - X_{i-1})$
61
MEMORIZZAZIONE X_i
62
$X_{CRI} = S_i x_{OR} X_i$
63
INVIO $X_{CR,i}$
64
SI
FINE BLOCCHI ?
NO
65
FINE

Fig.9

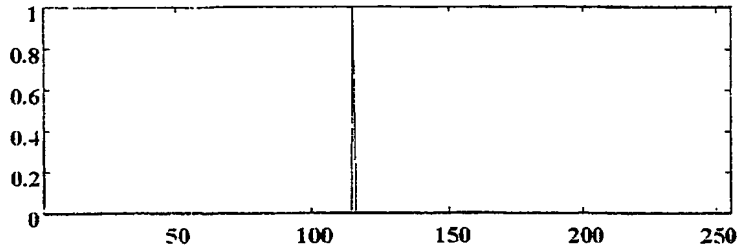


Fig.10a

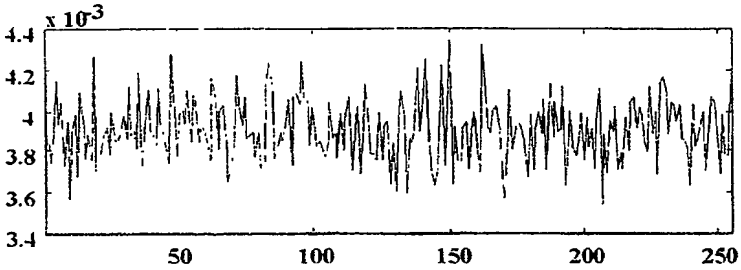


Fig.10b

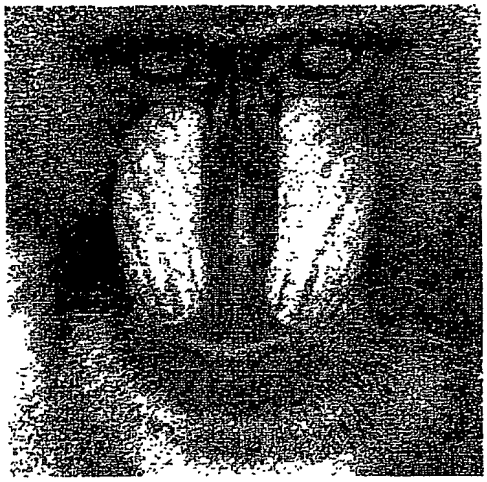


Fig.11a

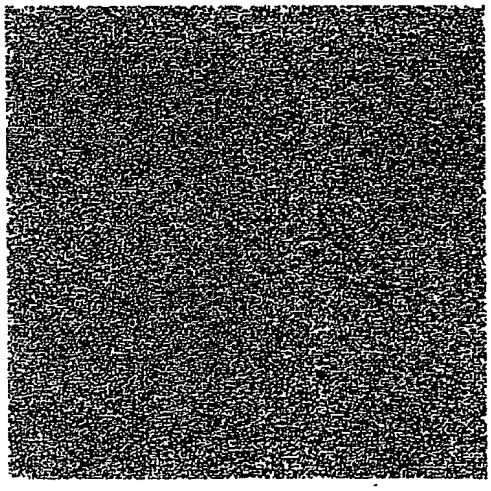


Fig.11b

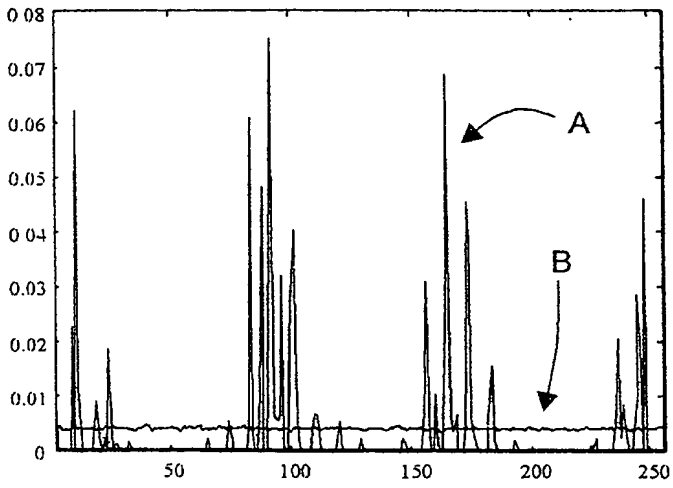


Fig.12